be protected is being provided without causing an electronic commerce operation being performed". And, it would also not be obvious to one with ordinary skill in the art to apply Haas et al. to Wiedemer as the existence of billing operation is already providing a better discouraging effect-it requires actual payment.

Accordingly, 103(a) rejection of claim 1 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

**Regarding claim 12 as amended**, it is equivalent to claim 1 as it requires "a processing apparatus having an identity software/means".

Therefore, if claim 1 as amended is allowable, then claim 12 as amended should be allowable as well. Accordingly, 103(a) rejection of claim 12 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

It further requires " the identity software/means being for providing a second information specific to a rightful user of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and the second information being for enabling electronic commerce operation(s) for which said rightful user has to be responsible". And, the extra limitation of "obtaining first information from a user" can be met by password entry or the like.

**Regarding claim 14 as amended**, it is equivalent to claim 1 in that it requires "authenticating an identity software/means", this implicitly requires "determining existence of the identity software/means" as claim1 does.

Therefore, if claim 1 as amended is allowable, then claim 14 as amended should be allowable as well. Accordingly, 103(a) rejection of claim 14 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

Respectfully submitted,
Ho Keung, Tse.

5

# Version with markings

Only claims 1-4, 6, 7, 9, 12-14, 16, 18, 19, 20, 21 and 22 are being amended and shown. The deleted parts are enclosed in square brackets [ ] and new added parts are underlined.

Claims 10, 11 have been canceled.

1.(Amended) A method for protecting software from unauthorised use, comprising the steps of:

determining if identity means/[information] <u>software,</u> is existing in a processing apparatus <u>under control of a user</u> ;

using [a favourable result of said determination] <u>said identity means/software being determined as existing</u> as a pre-condition for causing said processing apparatus to provide <u>said</u> user access to said software desired to be protected ;

wherein :

said identity [means/information, if so existing, being capable of being used in] <u>means/software being for</u> enabling electron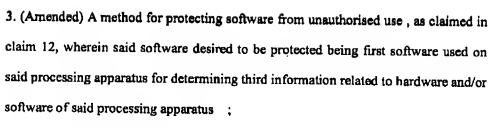ic commerce operation(s) for which <u>a</u> rightful [user(s)] <u>user</u> of said software desired to be protected has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/[information] <u>software</u> being specific to said rightful <u>user</u> [user(s) and said software desired to be protected being licensed to said rightful user(s)] .


2.(Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/[information] <u>software</u> ;

determining said identity means/[information] <u>software</u> as existing, if [the result of] said <u>identity means/software being determined as authentic</u> [authentication is favourable] and as not existing if otherwise .

3. (Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus    ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing user access to third software if said <u>computer being determined as authentic</u> [authentication result is favourable] .

4. (Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful [user(s)]<u>user</u> , <u>for obtaining a service/product</u>.

6. (Amended) A method for protecting software from unauthorised use, as claimed in claim 5, wherein <u>further comprising the steps of</u>:

[said processing apparatus having] <u>storing</u> an encrypted identity of [its rightful] <u>a</u> user <u>in said processing apparatus</u> ; and if [one] <u>all</u> of said protected programs stored in said processing apparatus has a valid user identity which being [not] consistent with the decryption result of said <u>stored</u> encrypted identity [of said processing apparatus], <u>permitting</u> use of said protected programs [will not be permitted] and [will be permitted] <u>not permitting</u> if otherwise .

7.(Amended) A computer software product for protecting software publicly distributed against unauthorised use   ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed ;

a computer readable medium having said identity program code and said authorising software ;

wherein :

said identity program code and said authorising software are [contained] stored in said [software product] medium in such a manner that said authorising software is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no specific hardware and/or software [specific to said rightful user(s)] other than said identity program code and said identity program code being specific to said rightful user(s) ;

[and said identity program code and said authorising software existing in a computer readable medium] .


9.(Amended) A computer software product as claimed in claim 7, wherein said authorising software contains said identity program code therein and said computer readable medium being in form of data signal embodied in a carrier wave.

12.(Amended) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software/means being for providing a second information specific to a rightful [user(s)] user of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being [capable of being used in] for enabling electronic commerce operation(s) for which said rightful [user(s)] user has to be responsible;

access to said software desired to be protected is being provided without causing a said operation being performed.


13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful [user(s)] user and said first information being a password.

14.(Amended) A method for protecting software from unauthorised use, comprising the steps of :

authenticating identity software[information]/means associated with a processing apparatus under control of a user ;

using [a favourable result of said authentication] said identity software/means being determined as authentic as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

wherein said identity [information/means existing in such a manner that said identity information/means being capable of being used in] software/means being for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity software[information]/means being specific to said rightful user(s) [and said software desired to be protected being licensed to said rightful user(s)].

16. (Amended) A method for protecting software from unauthorised use , comprising the steps of :

(a)   obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b)   determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

(c)   authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

(d)   using [a favourable result of said authentication] said second processing apparatus being determined as authentic as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

wherein said third information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible; and said method is being performed without causing a said transaction take place .

18.(Amended) A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a)    establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b)    verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being [obtained] communicated to said remote electronic transaction system from said processing apparatus ;

(c)    using [a favourable result of said verification] said account being determined as valid as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d)    authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e)    using [a favourable result of said authentication] said second processing apparatus being determined as authentic as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

19.(Amended) A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge [by said software distribution system] for repeating [at least] said sub-method [steps c] to e]] .

20.(Amended) A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use; comprising a sub-method;

wherein said sub-method a protection software being used and "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/means being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a)   determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step   (c) below ; thereafter

(b)   determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c)   determining if said second information is consistent with said first information ;

(d)   using [a favourable result of said determination of consistence] said second information being determined as consistence with said first information as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

21.(Amended) A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

[a)] receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

[b)] verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

[c)] using by said data processing apparatus, [a favourable result of said verification] said account being determined as valid as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said [steps a) to c) are] method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

22.(Amended) A software product comprising computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18 , 20 or 21 ;
[said computer code existing in] a computer readable medium having said computer code.

# Replace Sheets

All claims 1-9, 12-23 are shown, the sheet # shown at the top

indicates the sheet of the original filed SPEC to be replaced.

Claim 23 is new.

Claims 10, 11 have been canceled.

-7-

space, with a part B thereof being encrypted. As seen, the AS sub-program decrypts part B and stores the result which size should be not equivalent to that of the encrypted copy, in 'part B decrypted'.

The AS sub-program then overwrites at the first location of 'part B encrypted' an instruction 'JUMP TO part B decrypted' and at the end of 'part B decrypted' appends an instruction 'JUMP TO part C'. In this way, the encrypted part of the software will not be executed and the decrypted part will be executed instead.

In the case of audio/visual multimedia software, the software will be decrypted a small part by a small part and each small part is decrypted at the time it is about to be utilized by a audio/visual program for causing audio/visual effect. In other words, that audio/visual program has to cause the AS sub-program to be executed in the manner as described above in item 1b, everytime it wants a decryption of a small part. Desirably, a newly decrypted small part will overwrite a previously decrypted one so that a whole copy of the decrypted software will not exist in RAM.


4) The Sub-program for authenticating user computer (AC sub-program).

The AC sub-program for authenticating a computer on which it runs as being a particular predetermined computer, and prevent use of protected software if the computer is not, and its operation is under control of the central program.

Specifically, when the central program is being installed in a harddisk of a user computer and executed, it will check an encrypted status information stored in itself and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an encrypted identity of the rightful user of the central program, then the AC sub-program requests for an encrypted command from the central computer which will provide such an encrypted command, in the manner as described herein above in item 3i, if the rightful user has a valid account which is not closed.

-13-

1. A method for protecting software from unauthorised use, comprising the steps of:

     determining if identity means/software, is existing in a processing apparatus under control of a user ;

     using said identity means/software being determined as existing as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

     wherein :

     said identity means/software being for enabling electronic commerce operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

     access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/software being specific to said rightful user .


2. A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/software ;

determining said identity means/software as existing, if said identity means/software being determined as authentic and as not existing if otherwise .

-14-

3. A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus   ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing user access to third software if said computer being determined as authentic .

4. A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful user, for obtaining a service/product.

5. A method for protecting software from unauthorised use , as claimed in claim 1, wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

-15-

6. A method for protecting software from unauthorised use, as claimed in claim 5, wherein further comprising the steps of:

storing an encrypted identity of a user in said processing apparatus ; and if all of said protected programs stored in said processing apparatus has a valid user identity which being consistent with the decryption result of said stored encrypted identity, permitting use of said protected programs and not permitting if otherwise .


7. A computer software product for protecting software publicly distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed ;

a computer readable medium having said identity program code and said authorising software ;

wherein :

said identity program code and said authorising software are stored in said medium in such a manner that said authorising software is prevented from being copied therefrom individually; and

-16-

the improvement resides in said protection basing on no specific hardware and/or software other than said identity program code and said identity program code being specific to said rightful user(s).

8. A computer software product as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user(s).

9. A computer software product as claimed in claim 7, wherein said authorising software contains said identity program code therein and said computer readable medium being in form of data signal embodied in a carrier wave.

-17-

12. A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software/means being for providing a second information specific to a rightful user of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being for enabling electronic commerce operation(s) for which said rightful user has to be responsible;

access to said software desired to be protected is being provided without causing a said operation being performed.

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user and said first information being a password.

-18-

14. A method for protecting software from unauthorised use, comprising the steps of :

authenticating identity software/means associated with a processing apparatus under control of a user ;

using said identity software/means being determined as authentic as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

wherein said identity software/means being for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity software/means being specific to said rightful user(s).


15. A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

-19-

16. A method for protecting software from unauthorised use , comprising the steps of :

(a)  obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b)  determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

(c)  authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

(d)  using said second processing apparatus being determined as authentic as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

wherein said third information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible; and said method is being performed without causing a said transaction take place .

17. A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

-20-

18. A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a)    establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b)    verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being communicated to said remote electronic transaction system from said processing apparatus ;

(c)    using said account being determined as valid as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d)    authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e)    using said second processing apparatus being determined as authentic as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

-21-

19. A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge for repeating said sub-method .


20. A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use; comprising a sub-method;

wherein said sub-method a protection software being used and "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/means being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if said second information is consistent with said first information ;

-22-

(d) using said second Information being determined as consistence with said first information as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

21. A method for verifying Identity of a user of a data processing apparatus, comprising the steps of :

receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

using by said data processing apparatus, said account being determined as valid as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

-23-

22. A software product comprising computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18 , 20 or 21 ;

a computer readable medium having said computer code.


23. A software product as claimed by claim 22, wherein said computer readable medium being in the form of data signal embodied in a carrier wave.